UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

CHRISTINE REEVES, *also known as* CHRISTINE NEWMAN

and

VCARE USA LLC,

Defendants.

DECLARATION OF UNITED STATES POSTAL INSPECTOR THOMAS NINAN

I, Thomas Ninan, declare as follows:

1. I am a United States Postal Inspector and have been employed by the United States Postal Inspection Service ("USPIS") for more than 16 years. As a U.S. Postal Inspector, I am responsible for the investigation of violations of United States laws, including violations of Title 18 U.S.C. § 1341 (Mail Fraud), 18 U.S.C. § 1343 (Wire Fraud), and related statues of the United States Code. I am currently assigned to the Department of Justice International Fraud Team of the USPIS – Criminal Investigations Group, where my duties include investigating cases related to mail fraud and wire fraud, mass marketing schemes as well as telemarketing schemes. I have attended specialized training courses provided by the USPIS and the Department of Justice, including, Advanced Mail Fraud, Money Laundering and Asset Forfeiture. As a Postal

Inspector, I have conducted and I am presently conducting investigations into mass-marketing fraud schemes, including those perpetrated through telemarketing.

2. The facts set forth in this declaration are based on my personal knowledge, knowledge obtained during my participation in this investigation, information from other individuals including other law enforcement officers, victim interviews, and my review of documents, public records, and other sources. The major sources of evidence in this investigation include: Federal Trade Commission Consumer Sentinel Network complaints; victim complaints; and my review of business and public records; documents; and other sources. Because this affidavit is submitted for the limited purpose of supporting an application for a preliminary injunction, it does not set forth each and every fact that I learned during the course of this investigation.

3. Based on my training and experience and the facts as set for in this declaration, there is probable cause to believe that Christine Reeves and VCare USA LLC have committed and are committing violations of 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1956(a) (money laundering).

INVESTIGATION BACKGROUND

4. I am the lead United States Postal Inspector on an investigation into a fraudulent tech support scheme facilitated by Christine Reeves, through her company VCARE USA LLC, a company formed in Washington and, according to state corporation records, located in Gold Bar, Washington.

5. Defendant conducts U.S. operations of a technical-support scheme based in India that targets victims in the United States. The scheme fraudulently induces victims, to purchase bogus or otherwise misrepresented technical-support services related to computers or other

personal electronic devices and to make further payments based on additional fraudulent misrepresentations.

6. Reeves is a resident in the state of Washington with a residential address in Gold Bar, Washington.

7. VCare USA LLC is a Washington limited liability corporation with its primary address listed as 15606 Goldbar Drive, Gold Bar, Washington, 98251. Reeves formed the limited liability corporation in Washington in August 2016. VCare did not file its annual report last year, so the Washington Secretary of State administratively dissolved the LLC as of January 3, 2019. Reeves and VCare transact or have transacted business in this district and throughout the United States.

8. VCare and Reeves have and continue to participate in a large-scale technical-support fraud scheme based in India that targets consumers throughout the United States. Defendants further the scheme by receiving money from U.S. victims and then transmitting large sums of money obtained by fraud to accomplices in India and the United States, knowing that their transactions are designed to conceal the nature, source, location, ownership, and control of proceeds.

9. Since at least as early as 2016, telemarketers based in India have telephoned consumers in the United States and used the infrastructure maintained by Defendant to operate a technical support scheme. Telemarketers working for the scheme pose as purported technicians fraudulently to induce victims, including principally elderly victims, to purchase bogus or otherwise misrepresented technical support services and to make further payments based on additional fraudulent misrepresentations. Telemarketers contact victims either by cold-calling them, or by using pop-up advertisements disguised as security alerts on their computers or other electronic devices that direct victims to immediately call a telephone number to protect their

computers or other electronic devices. Telemarketers often falsely claim to work for or be affiliated with large, well-known technology companies such as Microsoft, Yahoo, and Google.

10. Regardless of the initial method of contacting a victim, the scheme proceeds similarly once a telemarketer working for the scheme has the consumer on the phone. Emphasizing the need for immediate action, the telemarketer claims that the consumer's computer is at risk and the telemarketer can assist the consumer but first needs remote access to the consumer's computer. Once remotely connected, the telemarketer purports to confirm the existence of a serious computer virus or other threat to the consumer's device. Sometimes the telemarketer claim that a hacker will soon be able to access the consumer personal information, including financial account numbers, social security numbers, and passwords. Imparting a sense of urgency, the telemarketer then claims that he will install expensive and high-quality network security software to resolve the threat in exchange for a substantial sum of money.

11. After the telemarketer purports to have installed high-quality network security software, he instructs the consumer to pay by check, money order, ACH, or wire.

12. At times during the scheme, victims who have already paid Defendant once for technical support receive subsequent calls from telemarketers working for the scheme, during which calls the telemarketers concoct new bogus reasons why the consumer must purchase additional security software to avoid new serious computer virus or other threat to the victim's device.

13. The fraud scheme charges its victims between $199.00 – $6,999, based on the telemarketer's ability to convince and defraud the victim.

14. One elderly victim in this scheme, Dr. Kenneth Dickie, was ultimately defrauded $89,999.98 through approximately several dozen separate transactions. Over seven months, from June 2017 to January 2018, Dr. Dickie transferred funds totaling these amounts:

VCare:	$ 20,400.00	
Reeves:	5,500.00	($3,000 of which were later reversed and returned)
Hites Technologies:	28,599.99	
Bhanu Pratap:	11,500.00	
Itess Technologies and Itess Global:	7,500.00	
Subtotal:	$ 73,499.99	
1 Stop Solutions LLC:	15,000.00	
Click IT Solution:	1,499.99	
Total:	$ 89,999.98	

15. Reeves and VCare have transferred considerable amounts of money to accomplices in India. From September 2016 through June 2018 alone, Reeves wired at least $70,000 from VCare business accounts to Itess Technologies accounts in India.

16. One bank official's internal record typifies Reeves' and VCare's activities: "Business account is funded by checks from makers in different states, all appear to come from elderly customer [*sic*] with memos 'computer', 'computer support', 'computer services' * * * Immediate use of funds by outgoing wires to India totaling $51,000 since 05/01/18." This bank record was dated just two months later, on June 28, 2018.

17. At times, Reeves has made frequent and large cash withdrawals from VCare business accounts. Over the six and a half weeks from December 23, 2017, to February 11, 2018, Reeves withdrew at least $25,000 in at least 33 different cash withdrawals from a single account. These included two counter withdrawals of $5,000 and $6,000 less than a week apart in mid-January 2018, as well as 31 separate ATM withdrawals totaling $14,000.

18. The Federal Trade Commission maintains a database of consumer complaints, known as Consumer Sentinel. As of February 25, 2019, there were 12 Consumer Sentinel complaints filed about VCare USA LLC, Christine Reeves, or the toll-free numbers most often reported for VCare and Reeves (800-935-1758 and 866-663-1666). The complaints describe how consumers have received calls stating that they are from Yahoo or Google, or are Microsoft-

certified technicians, and that the company was informed that the consumer's computer is full of malicious viruses. The complaints go on to explain that the caller goes on to seek permission to remotely access the consumer's computer and remedy the situation.

19. In 2016, a VCare and Reeves accomplice based in India named Bhanu Pratap registered VCare's website and email domain name: "vcareusallc.com". The website has recently been taken down, but while functional, it explained that VCare provided computer technical services. Its "Contact Us" page listed VCare's street address, as the same Gold Bar, Washington, address where Reeves lived. The "Terms and Conditions" page on the VCare website repeatedly referenced another VCare accomplice, Hites Technologies. The absence of spaces after "Hites Technologies," and after the last reference to "VCare USA LLC" in the final line below, suggests that VCare's website was copied and pasted from a template also used to create web material for Hites Technologies. The relevant language from the "Terms and Conditions" page reads:

> **Vcare USA LLC** [Tr]ademark "Hites Technologies" is used by Vcare USA LLC
>
> **"Hites Technologies Certified Technician/(s)"** "Vcare USA LLC Certified Technician means" technicians and specialists certified by Hites Technologiesto perform the Services under this Agreement.
>
> **"Subscription Based Plans"** "Subscription Based Plans" or "Subscription/(s)" are tenured Subscription plans offered by Vcare USA LLC that are active for a specified period and will not include any incident based plans such as "Per Incident Plan" or the like.
>
> **"Services" AND "Hites Technologies Portal"** All references to "Services" refer to any Vcare USA LLC service delivered through Hites TechnologiesTechnical Services Private Limited, under the plan that you enter into with Hites TechnologiesLLC through use of the Hites TechnologiesWebsite located at www.hitesav.com (the "Hites TechnologiesPortal") or by calling the Hites TechnologiesLLC phone number mentioned on the Hites TechnologiesWebsite. These Terms of Use govern all plans available through the Vcare USA LLC Website, and any use of the Hites TechnologiesPortal. In the event of any conflict these Terms of Use control any valid Plan Order form that you submit requesting Services ("Plan Order").
>
> **"Materials"** "Materials" means any web casts, download areas, white papers, press releases, datasheets, FAQs, product information, quick reference guides, or other works of any kind that are made available to download from the Vcare USA LLC Portal are the proprietary and copyrighted work of Hites Technologiesand/or its suppliers. The definition of "Materials"

does not include the design or layout of the Vcare USA LLC.net web site or any other Vcare USA LLCowned, operated, licensed or controlled website.

20. "Returned deposits" are deposits that a financial institution returns as unpayable for various reasons. Among the reasons deposits may be returned are instances where the maker of a check has placed a stop-payment order on the check or the sender seeks to reverse a bank wire. Additionally retuned deposits can result from the closure of a victim's bank account by financial institutions that receive complaints of fraud from the victim.

21. Since Reeves formed VCare as a single-member LLC in August 2016, she has opened business accounts for VCare at seven or more banks. At least six of these banks have force-closed VCare business accounts due to suspected fraud (based on high rates of returned deposits, fraud reports from victims trying to stop payment, or both). At least one bank concurrently force-closed Reeves' personal bank account for the same reason. Separate from the banks, an Internet-based crypto-currency exchange that Reeves used to transmit money to Bhanu Pratap (an accomplice in India) was also force-closed because she made deposits that were returned as worthless.

22. In mid-March 2018, an official at one of VCare's banks contacted Reeves for additional information regarding VCare and the activity in its bank account. When I interviewed the bank official on September 24, 2018, as part of this investigation, she advised that Reeves was very vague and not forthcoming in her responses. The bank official related that she informed Reeves that the bank would be closing VCare's bank account because it was being used to support a computer tech scam and that the bank suspected Reeves was working in concert with other individuals in the fraud.

23. VCare and Reeves' conduct has continued unabated since the bank official's mid-March 2018 conversation with Reeves. More than half of the Consumer Sentinel Network

complaints about VCare and Reeves concern transactions that post-date that conversation. Within two weeks of that conversation, Reeves had opened a new business account for VCare at a new bank; that business account, too, was closed by the end of May 2018 for suspected fraud.

24. Meanwhile, during May and June 2018, VCare sent nine bank wires to India, totaling $51,000, from another VCare business account that Reeves opened at a different bank. From late April to the end of June 2018, seven checks deposited into that VCare business account and into a personal account Reeves held at the same bank were returned as unpayable.

25. As part of my investigation, I tried contacting Reeves and left her messages on January 15, 2019, saying I wanted to speak with her, but did not hear back from her.

Pursuant to 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed on March 5, 2019 in Washington, DC

Thomas Ninan
Postal Inspector
United States Postal Inspection Service